US 20150281003A1

(19) **United States**

(12) **Patent Application Publication**

Peterson et al.

(10) **Pub. No.: US 2015/0281003 A1**

(43) **Pub. Date: Oct. 1, 2015**

(54) **MOBILE APPLICATION CONTROL**

(71) Applicant: **SonicWALL, Inc.**, San Jose, CA (US)

(72) Inventors: **Chris D. Peterson**, Bellingham, WA (US); **Praveen Kumar**, Kirkland, WA (US)

(21) Appl. No.: **14/319,166**

(22) Filed: **Jun. 30, 2014**

Related U.S. Application Data

(60) Provisional application No. 61/973,248, filed on Mar. 31, 2014.

Publication Classification

(51) **Int. Cl.**

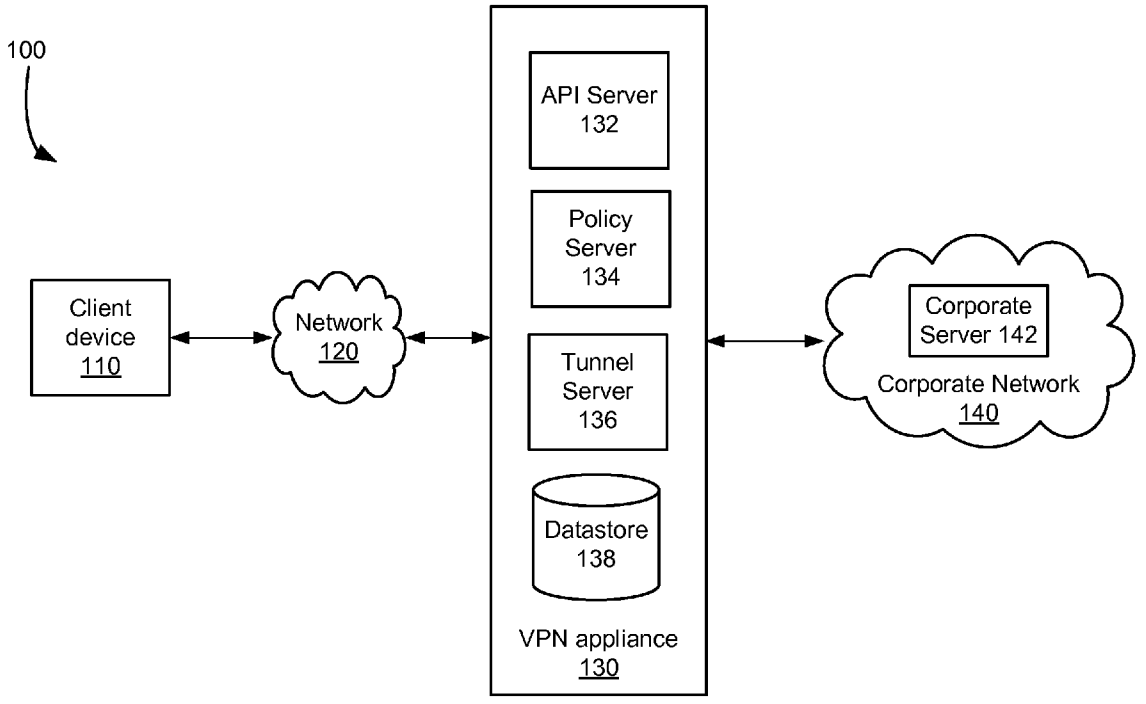
H04L 12/24	(2006.01)
H04L 29/06	(2006.01)
H04L 29/08	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 41/5006*** (2013.01); ***H04L 67/141*** (2013.01); ***H04L 63/0272*** (2013.01)

(57) **ABSTRACT**

A device user may determine what applications from a set of applications may access the corporate network and which applications do not access the network. An indication of the limits on what a corporate network may access on a user personal device may provided to a user and either accepted or rejected. The user, if the user agreement is accepted, may receive a list of allowed applications and modify the list by removing applications on the list which the user does not want to send data to the corporate network. Both the user and a corporate network administrator may view the user accepted limits and track what user device applications actually have accessed the corporate network to confirm compliance with the limits.



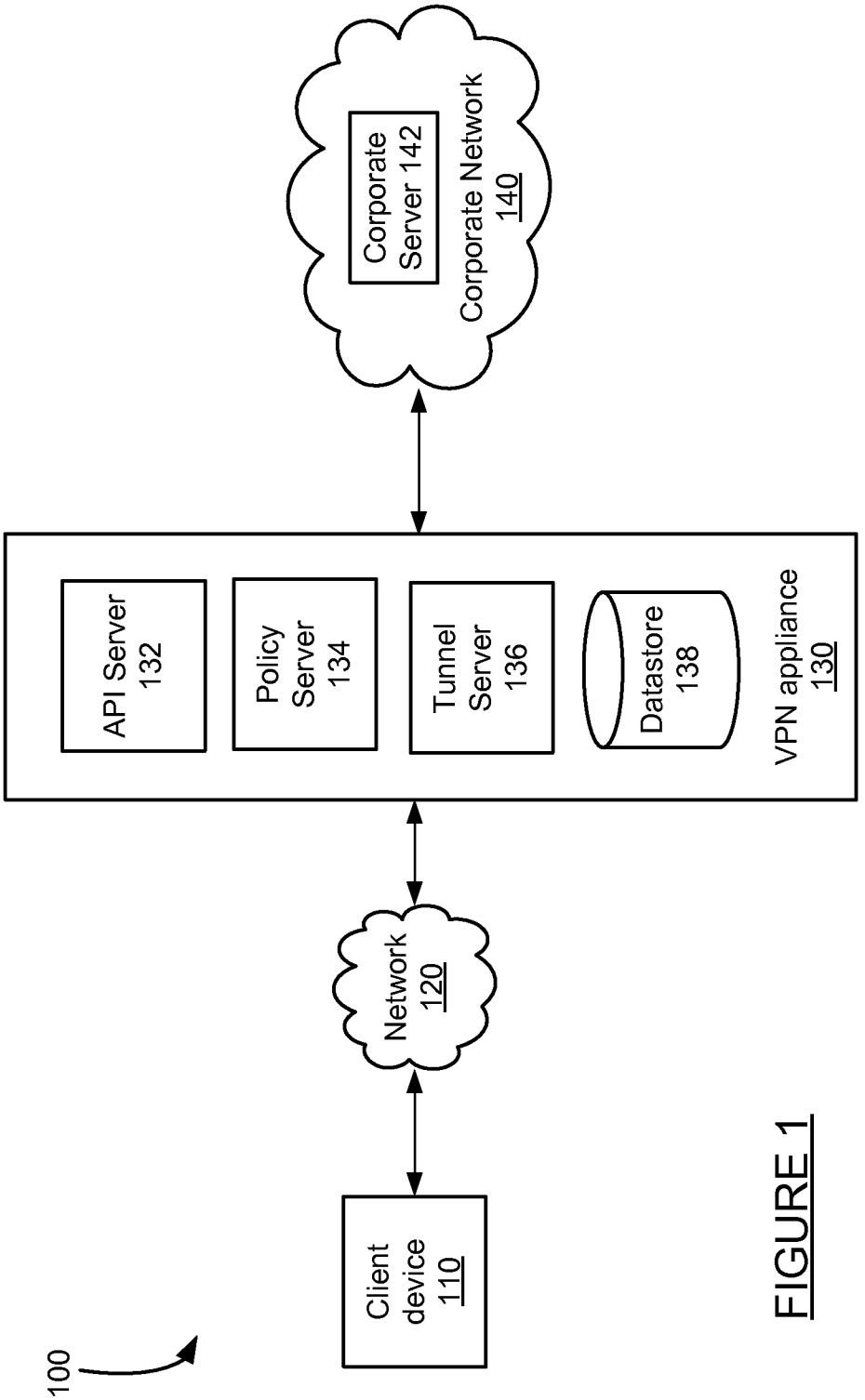

Corporate Server 142
Corporate Network 140
API Server 132
Policy Server 134
Tunnel Server 136
Datastore 138
VPN appliance 130
Network 120
Client device 110
100

FIGURE 1

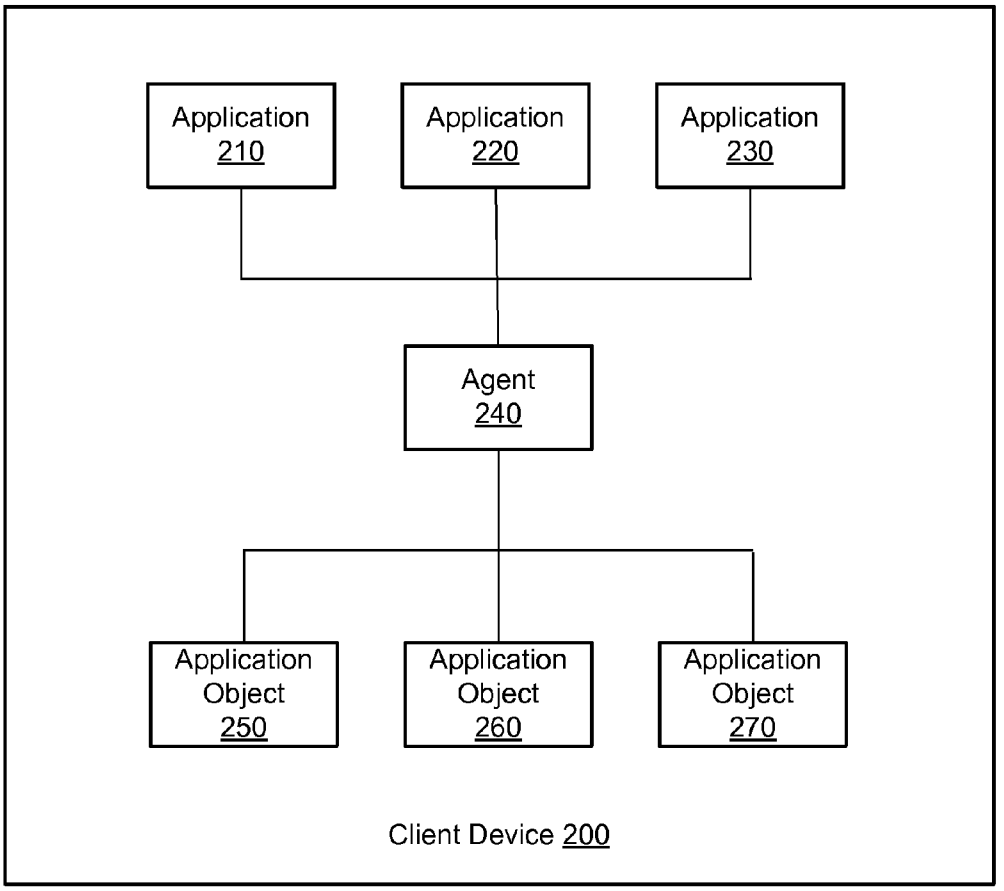

Application 210
Application 220
Application 230
Agent 240
Application Object 250
Application Object 260
Application Object 270
Client Device 200

FIGURE 2

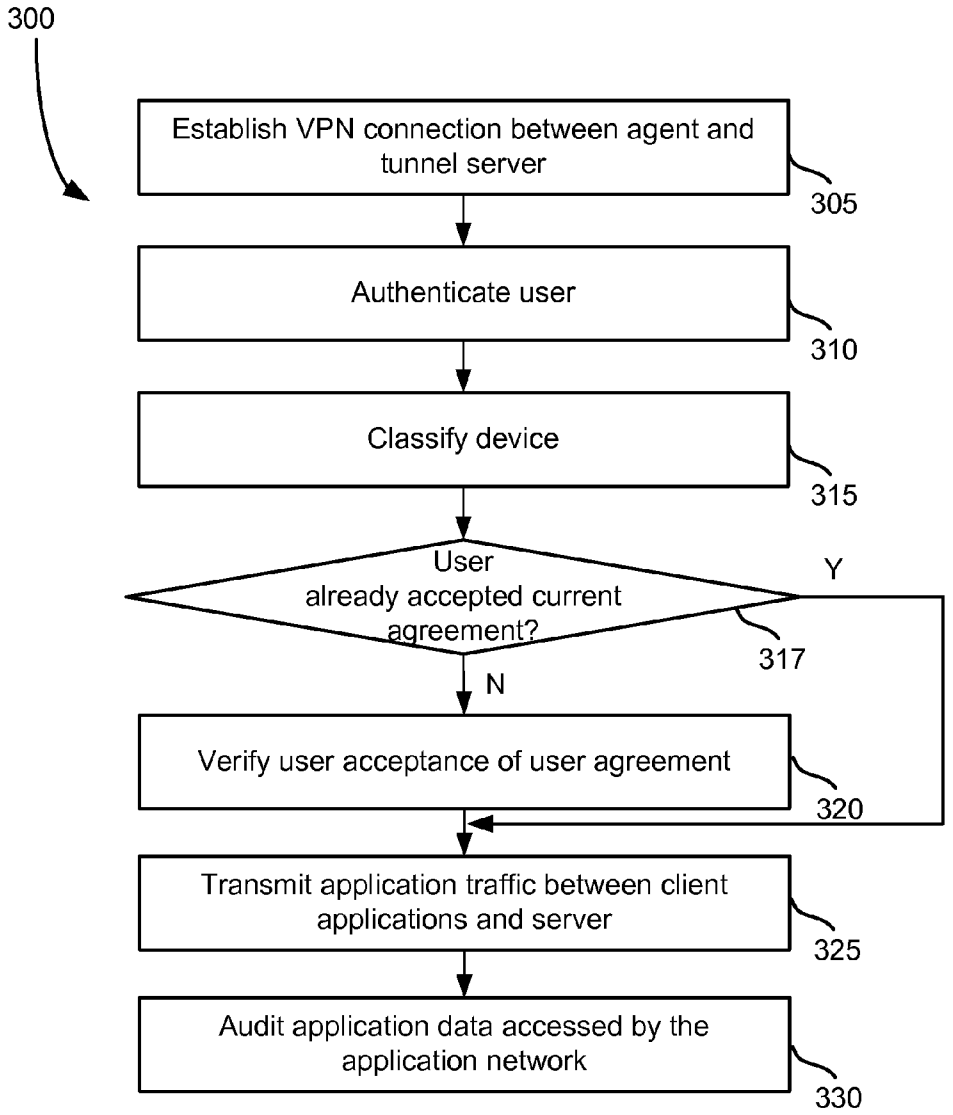

300
Establish VPN connection between agent and tunnel server
305
Authenticate user
310
Classify device
315
User already accepted current agreement?
317
Y
N
Verify user acceptance of user agreement
320
Transmit application traffic between client applications and server
325
Audit application data accessed by the application network
330

FIGURE 3

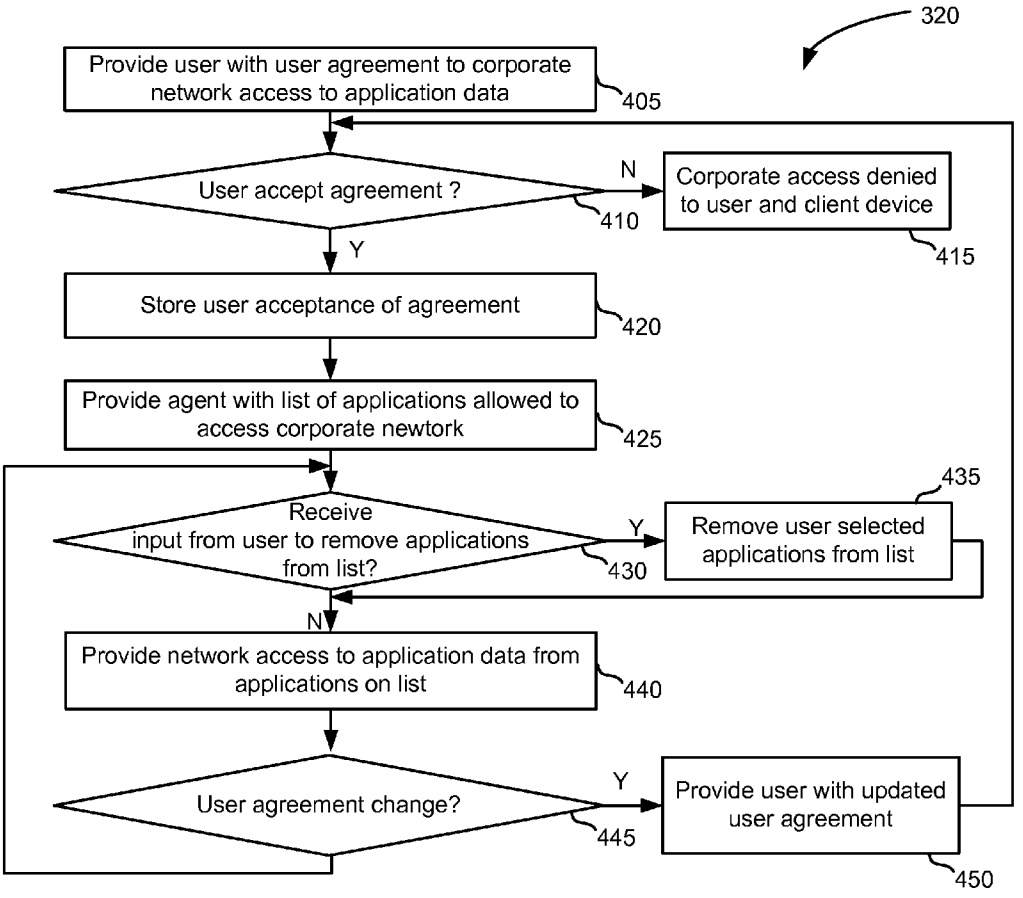

320
Provide user with user agreement to corporate network access to application data
405
User accept agreement ?
410
N
Corporate access denied to user and client device
415
Y
Store user acceptance of agreement
420
Provide agent with list of applications allowed to access corporate newtork
425
Receive input from user to remove applications from list?
430
Y
435
Remove user selected applications from list
N
Provide network access to application data from applications on list
440
User agreement change?
445
Y
Provide user with updated user agreement
450

FIGURE 4

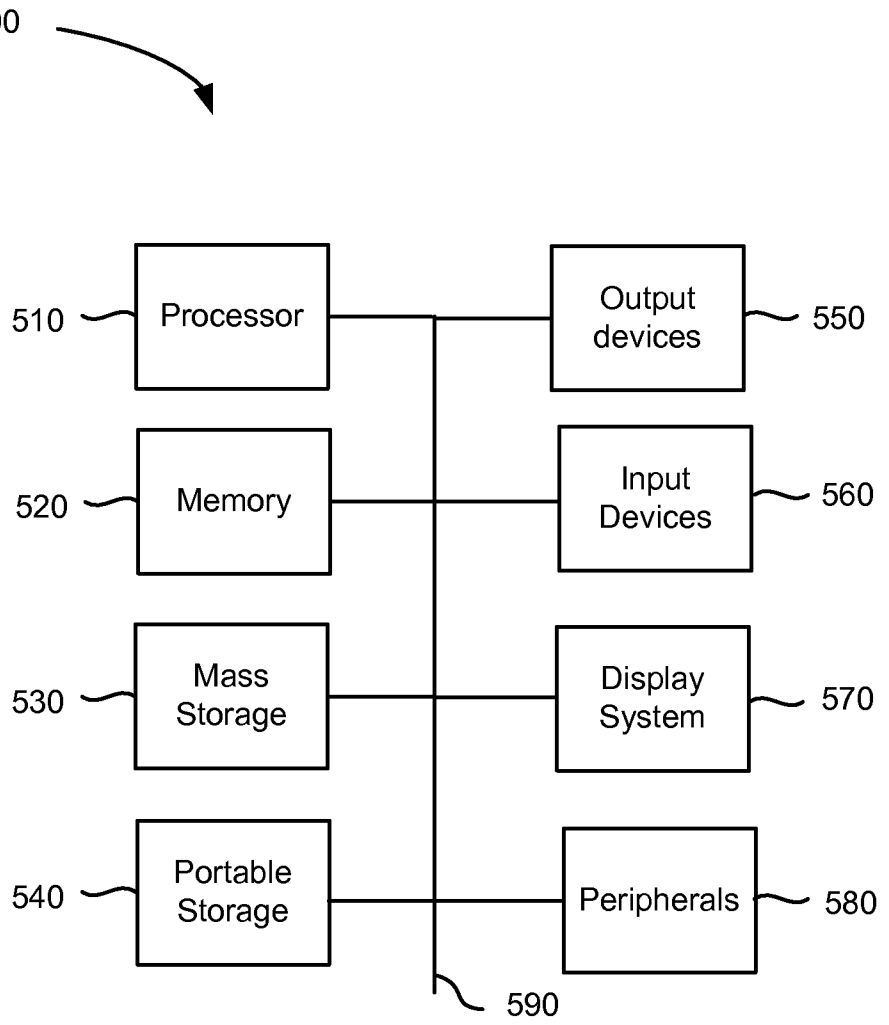

500
510
Processor
520
Memory
530
Mass Storage
540
Portable Storage
Output devices
550
Input Devices
560
Display System
570
Peripherals
580
590

FIGURE 5

MOBILE APPLICATION CONTROL

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the priority benefit of U.S. Provisional Application Ser. No. 61/973,248, titled "Mobile Connect," filed Mar. 31, 2014, the disclosure of which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] Consumers continue to push for a mechanism that allows them to use their own device to perform typical work tasks. In most cases, these devices are owned by the individual user, which means the company may have zero control over them. Because companies have little if any control over these user devices, there is concern regarding providing the device access to corporate remote networks due to the potential for attacks vectors (nefarious applications, leaking, tampering, or otherwise disclosing of critical intellectual property owned by company). The market has coined the term "unmanaged device" or "BYOD" (bring your own device) to represent any device that is not owned or controlled by the company that needs access to the corporate network so the employee can do their work. In most cases, this device is owned by the employee requesting access. Some companies require employee devices to be put under mobile device management (MDM) control before allowed onto the corporate network, but such a configuration is not really zero control.

[0003] Most mobile solutions are all or nothing—all data is shared or no data is shared with respect to a corporate intranet (i.e., an appliance based network). With the advent of BYOD, users need to access the corporate intranet but do not want their personal information to be available to the corporate intranet. Likewise, the corporate intranet may not want to risk exposure to certain content on the user device that is not germane (or appropriate) for the corporate network.

[0004] Secure communication with a corporate network can be achieved through virtual private network (VPN) connections. Current VPN clients that provide application level control block traffic in that VPN application running on the client device. For example, some companies provide a per-app VPN solution. Despite current VPN per application solutions, there are still concerns regarding the vulnerability of corporate network access from personal user devices.

[0005] There is a need in the art for managing access to corporate networks by user's personal devices at the application level that protects corporate interests while protecting personal data of users.

SUMMARY OF THE CLAIMED INVENTION

[0006] An appliance works in conjunction with an agent on a remote device to control application access to a corporate network. In conjunction with an SSL tunnel and policy operating at the appliance, granular application control may be implemented. In particular, a device user may determine what applications from a set of applications may access the corporate network and which applications do not access the network. A user agreement indicating of the limits on what a corporate network may access on a user personal device may be provided to a user and either accepted or rejected. The user, if the user agreement is accepted, may receive a list of allowed applications and modify the list by removing applications on the list which the user does not want to send data to the corporate network. Both the user and a corporate network administrator may view the user accepted limits and track what user device applications actually have accessed the corporate network to confirm compliance with the limits.

[0007] An embodiment may include a method for establishing a connection. The method may include establishing a connection between a user client device and a server. The user client device may have a plurality of applications and be associated with a user. A user agreement regarding what a corporate network will access on the user client device may be presented to the user through the user client device and from the server. A confirmation may be received of the user agreement from the user by the client device. The client may be provided with access to the corporate network by the server.

[0008] In an embodiment, a system for establishing a connection may include a device having a processor, memory, and an agent stored in memory and executable by the processor to establish a connection between a user client device and a server, the user client device having a plurality of applications and associated with a user, present to the user through the user client device a user agreement on what a corporate network will access on the user client device, receive a confirmation of the user agreement from the user by the client device, and provide the client access to the corporate network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. **1** illustrates a block diagram of a client communicating with a remote server.

[0010] FIG. **2** illustrates a block diagram of a client having an agent.

[0011] FIG. **3** illustrates a method for providing application access to a network.

[0012] FIG. **4** illustrates a method for verifying user acceptance of a user agreement.

[0013] FIG. **5** is a block diagram of an exemplary system for implementing a computing device.

DETAILED DESCRIPTION

[0014] An intranet appliance works in conjunction with an agent on a remote device to control application access to a corporate network. In conjunction with an SSL tunnel and policy operating at the appliance, granular application control may be implemented. In particular, a device user may determine what applications from a set of applications may access the corporate network and which applications do not access the network.

[0015] A device user may determine what applications from a set of applications may access the corporate network and which applications do not access the network. A user agreement indicating what a corporate network may access on a user personal device may provided to a user and either accepted or rejected. The user, if the user agreement is accepted, may receive a list of allowed applications and modify the list by removing applications on the list which the user does not want to send data to the corporate network. Both the user and a corporate network administrator may view the user accepted limits and track what user device applications actually have accessed the corporate network to confirm compliance with the limits.

[0016] FIG. **1** illustrates a block diagram of a client communicating with a remote server. The system of FIG. **1** includes client device **110**, network **120**, VPN appliance **130**,

and corporate network **140**. VPN appliance **130** may include tunnel server **136**, policy server **134**, and data store **138**. Corporate network **140** may include one or more servers such as corporate server **142**.

[0017] Client **110** may include a user device that is not controlled by the entity that provides **1 1** corporate network **140**. Client **110** may be implemented as a mobile device such as a smart phone, tablet or laptop computer, a desk top computer, or other computing device.

[0018] Network **120** may include one or more networks used to communicate data between client device **120** and, ultimately, corporate server **142**. For example, network **120** may include a private network, public network, the Internet, an intranet, a local area network, a wide area network, a wireless network, a cellular network, and a combination of these networks.

[0019] Tunnel server **130** on VPN appliance **125** may establish a VPN tunnel and communicate with client device **110** and serve as an intermediary between client device **110** and corporate server **142**. This VPN may be used to allow applications on the client device **110** to communicate with a corporate server **142** in a secure fashion even though traffic is flowing over a public network **120**.

[0020] 1The policy server may include one or more applications that perform functionality discussed herein, such as for example generating and applying policy rules. Datastore **138** may store and process data, and is accessible by servers **132**, **134** and **136**. For example, datastore **138** may store communication log data, application lists, application information, and other data. The client device **110** may communicate with tunnel server **136** to authorize access to corporate server **142**. The client may also communicate through an API Server **132** which is a peer to the tunnel server and is used to authenticate the user, retrieve the list of applications, authenticate a device, and other functionality. Both API Server **132** and Tunnel Server **136** may communicate with policy server **134** to obtain policy decisions to help provide responses to client requests

[0021] Corporate server **142** of corporate network **140** may be accessed by the user device **110** through tunnel server **136** of VPN appliance **130**. In this case, tunnel server **136** may receive and analyze all network traffic to confirm the traffic is from an authorized application before the traffic may access the corporate server. Access to corporate server **142** and other resources on corporate network **140** is determined by both policy server **134** and tunnel server **136**. Tunnel Server **136** provides policy enforcement and traffic analysis while policy server **134** is the policy decision point, and the two servers work in concert to both analyze traffic and apply policy.

[0022] FIG. **2** illustrates a block diagram of a client having an agent. Agent **240** may communicate with tunnel sever **230** and API Server **280** to implement client side functionality of the present technology. For example, agent **240** may provide an interface to a user for selecting one or more of a set of applications allowed to access the corporate network **140**, collect data at the device and provide the data to tunnel server **136** or API server **132**, and other functionality.

[0023] Agent **240** may communicate with applications **210-230** on device **110** and may generate and manage application objects **250-260**. An application may correspond to each application object. An application object may include the application name, version, and other data for a corresponding application. Agent **240** may transmit application information within each application object to tunnel server **136** or API server **132** to allow policy server **134** to make access control decisions.

[0024] FIG. **3** illustrates a method for providing application access to a network. A VPN connection is established between the tunnel server and an agent **240** on the client at step **310**. The agent may initiate the VPN establishment by sending a VPN request to the VPN appliance.

[0025] A user is authenticated at step **310**. User authentication is performed to identify the user of the device. A user device is then classified to determine if it meets acceptable parameters at step **315**. In some instances, an administrator defines a set of device attributes, and the system may attempt to find a set of attributes that match the device. Classification of the device may include retrieval of a unique equipment identifier along with other device attribute data. The unique equipment identifier and device attribute data may be collected by an agent and transmitted to policy server **134**. The attribute data may be used by the policy server to determine if client device **110** may allow for application control by the policy server via the agent.

[0026] Once the user is authenticated and the device is classified, the data store is queried to determine if a matching entry for the user and device exist. If the user and device combination are found in the data store, then the user and device have established a connection with the corporate network before and the version of the user agreement previously agreed to by the user is checked against the most recent version at step **317**. If the user has already accepted the current user agreement at step **317**, and therefore the most recent user agreement has not changed from the stored user agreement for the user and device combination, then the method continues to step **325** and the present system does not provide the user with the same user agreement and a portion of or all of step **320** (and corresponding method of FIG. **4**) will not per performed for the current session.

[0027] If the device requires a new user agreement to be accepted, either because the user and device combination is not found in the data store or the current version of the user agreement does not match the stored version of the user agreement, the method continues from step **317** to step **320**.

[0028] User acceptance of a user agreement is verified at step **320**. Once a user accepts a user agreement, the user may be authorized for the corporate network access. In some embodiments, a policy server determines authorization of the user, device, and checks access permissions. The policy allows for application access to particular data for a particular device type and user type. Once the user has accepted the user agreement, the user may be authorized to access a corporate network. More detail for user acceptance of the user agreement is provided with respect to FIG. **4**.

[0029] Application traffic may be transmitted to the corporate network at step **325**. An agent on the client device may monitor communication data and provide information to the user of the device regarding what applications are communicating with the corporate network.

[0030] An audit may be performed on the application data sent to the corporate network at step **330**. The server will collect data as packets are transmitted to the corporate network regarding which user and device are sending traffic. The data may include an application identifier and version specific hash, which is collected for any application that sends data to the corporate network. The server may receive the data and

store the data for each session between the user and device combination and the corporate network.

[0031] The administrator may access the stored session data on the VPN appliance and identify which applications on the particular user device and for a particular user have sent data to the corporate network. The user may access data stored by the agent on the client device to identify which applications have sent data to which destination on the corporate network. The user and administrator may also access the limits agreed to by the user regarding application data to be sent to the corporate network. From this information, the user or administrator may each determine whether the application data transmitted complied with the limits agreed to by the user, thereby auditing the application data access by the corporate network.

[0032] FIG. **4** illustrates a method for verifying user acceptance of a user agreement. The method of FIG. **4** provides more detail for step **325** of the method of FIG. **3**. A user is provided with a user agreement regarding corporate network access to application data from applications on the user's device at step **405**. The user agreement is a mutual contract between the corporate network operator and the end user where the end user can choose to accept it to be granted access to the corporate network or decline and end their session. The language contained within the user agreement may be drafted by the corporate network legal counsel.

[0033] The user agreement may specify policies and rules regarding how the network access may access data, when it may access data, and generally inform the user of application data access over the corporate network. In some instances, the user agreement may be a contract offer to the user. The indication received by the user device from a server and provided to the user through an interface of the user device. A determination is then made as to whether the user accepts the user agreement at step **410**. If the user does not accept the limits indicated, access to a corporate access is denied to the user and user device combination at step **415**. If the user has not accepted the user agreement, upon a subsequent login attempt, the user may again be prompted to comply with the user agreement. If the user does accept the limits, the user's acceptance of the limits and the indication of the limits are stored at step **420**. If the user accepts the user agreement a copy of the user agreement is stored on the client device. A record for the user, device and user agreement version number may also be created or updated at the VPN appliance to reflect the user's acceptance. The user's acceptance will not be required from the user again for the same user agreement for the particular user and user device combination.

[0034] The agent on the client device is provided with a list of applications from the VPN appliance, wherein the listed applications are allowed to access the corporate network at step **425**. The list of applications is determined by the access policy configured by an administrator which contains detailed information on which users, devices, applications, and destinations should be granted access. If the received application list is the same list as that received during the previous session, the agent does nothing (e.g., will not present the newly received list to the user) and the method of FIG. **4** continues to step **440** (i.e., no input is received from the user as no applications from the newly received list are provided to the user).

[0035] If the list is different from the previous session for the user and device, or the list is provided during the first session for the user and device combination, the agent on the client device presents the list of applications to the user via an interface of the device. The user may choose to block applications on this list from accessing the corporate network and have network traffic data flow over the VPN. For each application, the application type may be specified along with particular versions or configurations of the application that may be allowed to access the corporate network. A determination is then made as to whether input is received from the user to remove applications from the list at step **430**. If such input is received, the user selected applications are removed from the list at step **435** and the method continues to step **440**. In some instances, if the user removes all the applications from the list, the session may be terminated. Otherwise, network access may be provided to application data from applications on the list at step **440**. At any time during the session, the user may change the applications on the current list which are authorized to send data to the corporate server.

[0036] If the user removes an application from the list by deselecting it, the client device will not send traffic from that application to the corporate network. A network administrator may not be notified that the user chose to limit the application set to less than what was authorized by the network administrator. Hence, what the user decides to allow or not allow with the company to use on their device is not shared with the network administrator. For example, if the user would like to user a particular network browser to access monster.com to look for a new job, the user likely will not want to have to explain to her supervisor why they disabled it.

[0037] At any time during the current session, a network administrator may access the version number of the user agreement accepted by the user, as this information is stored in the data store **138**. The user may also access a copy of the user agreement that they have previously agreed to, and may access a copy which has been stored on their device. The user may access a copy at any time via a menu setting on a UI provided by the VPN agent **240**.

[0038] FIG. **5** is a block diagram of an exemplary system for implementing a computing device. System **500** of FIG. **5** may be implemented in the contexts of the likes of client device **110** VPN appliance **130** and corporate server **140**. The computing system **500** of FIG. **5** includes one or more processors **510** and memory **520**. Main memory **510** stores, in part, instructions and data for execution by processor **510**. Main memory **520** can store the executable code when in operation. The system **500** of FIG. **5** further includes a mass storage device **530**, portable storage medium drive(s) **540**, output devices **550**, user input devices **560**, a graphics display **570**, and peripheral devices **580**.

[0039] The components shown in FIG. **5** are depicted as being connected via a single bus **590**. However, the components may be connected through one or more data transport means. For example, processor unit **510** and main memory **520** may be connected via a local microprocessor bus, and the mass storage device **530**, peripheral device(s) **580**, portable storage device **540**, and display system **570** may be connected via one or more input/output (I/O) buses.

[0040] Mass storage device **530**, which may be implemented with a magnetic disk drive or an optical disk drive, is a non-volatile storage device for storing data and instructions for use by processor unit **510**. Mass storage device **530** can store the system software for implementing embodiments of the present invention for purposes of loading that software into main memory **520**.

[0041] Portable storage device **540** operates in conjunction with a portable non-volatile storage medium, such as a floppy disk, compact disk or Digital video disc, to input and output data and code to and from the computer system **500** of FIG. **5**. The system software for implementing embodiments of the present invention may be stored on such a portable medium and input to the computer system **500** via the portable storage device **540**.

[0042] Input devices **560** provide a portion of a user interface. Input devices **560** may include an alpha-numeric keypad, such as a keyboard, for inputting alpha-numeric and other information, or a pointing device, such as a mouse, a trackball, stylus, or cursor direction keys. Additionally, the system **500** as shown in FIG. **5** includes output devices **550**. Examples of suitable output devices include speakers, printers, network interfaces, and monitors.

[0043] Display system **570** may include a liquid crystal display (LCD) or other suitable display device. Display system **570** receives textual and graphical information, and processes the information for output to the display device.

[0044] Peripherals **580** may include any type of computer support device to add additional functionality to the computer system. For example, peripheral device(s) **580** may include a modem or a router.

[0045] The components contained in the computer system **500** of FIG. **5** are those typically found in computer systems that may be suitable for use with embodiments of the present invention and are intended to represent a broad category of such computer components that are well known in the art. Thus, the computer system **500** of FIG. **5** can be a personal computer, hand held computing device, telephone, mobile computing device, workstation, server, minicomputer, mainframe computer, or any other computing device. The computer can also include different bus configurations, networked platforms, multi-processor platforms, etc. Various operating systems can be used including Unix, Linux, Windows, Macintosh OS, Palm OS, and other suitable operating systems.

[0046] The foregoing detailed description of the technology herein has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the technology to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. The described embodiments were chosen in order to best explain the principles of the technology and its practical application to thereby enable others skilled in the art to best utilize the technology in various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the technology be defined by the claims appended hereto. [0036-0044 look like boilerplate to me, did not bother checking them closely.]

What is claimed is:

1. A method for establishing a connection, comprising:

establishing a connection between a user client device and a server, the user client device having a plurality of applications and associated with a user;

presenting to the user through the user client device and from the server user agreement on what a corporate network will access on the user client device;

receiving a confirmation of the user agreement from the user by the client device; and

providing the client access to the corporate network by the server.

2. The method of claim **1**, further comprising generating the user agreement for the user and user client device combination.

3. The method of claim **1**, further comprising storing the user acceptance of the user agreement for the user and user client device combination.

4. The method of claim **1**, further comprising providing the user agreement to the user subsequent to the providing the client access to the corporate network.

5. The method of claim **1**, further comprising:

receiving login information from the user by the server via the user client device;

determining if the limits on what a corporate network will access on the user client device has changed;

providing an updated version of the limits on what a corporate network will access on the user client device; and

providing the client access to the corporate network by the server once the user has accepted the updated version of the limits on what a corporate network will access on the user client device.

6. The method of claim **1**, further comprising:

providing the user with information regarding what applications have sent data to the corporate network; and

providing an indication of compliance to the user regarding whether the data sent by the applications complies with the user agreement on what a corporate network will access on the user client device.

7. The method of claim **1**, further comprising:

providing an administrator of the corporate network with information regarding what applications have sent data to the corporate network; and

providing an indication of compliance to the administrator regarding whether the data sent by the applications complies with the user agreement on what a corporate network will access on the user client device.

8. The method of claim **1**, further comprising providing a list of applications allowed to access the corporate network to the user, the list provided from the server to the user through the user client device.

9. The method of claim **8**, further comprising receiving input from the user to select a subset of the list of applications to access the corporate network, wherein the one or more applications not selected by the user are blocked access to the corporate network.

10. The method of claim **8**, wherein the list is provided to the user at the start of the connection between the user client device and the server.

11. The method of claim **10**, further comprising:

detecting during the connection a change to the list of applications allowed to access the corporate network; and

providing the user with an updated list of applications allowed to access the corporate network.

12. A non-transitory computer readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for establishing a connection, the method comprising:

establishing a connection between a user client device and a server, the user client device having a plurality of applications and associated with a user;

presenting to the user through the user client device user agreement on what a corporate network will access on the user client device;

receiving a confirmation of the user agreement from the user by the client device; and

providing the client access to the corporate network.

13. The non-transitory computer readable storage medium of claim **12**, further comprising generating the user agreement for the user and user client device combination.

14. The non-transitory computer readable storage medium of claim **12**, further comprising storing the user acceptance of the user agreement for the user and user client device combination.

15. The non-transitory computer readable storage medium of claim **12**, further comprising providing the user agreement to the user subsequent to the providing the client access to the corporate network.

16. The non-transitory computer readable storage medium of claim **12**, further comprising:

receiving login information from the user by the server via the user client device;

determining if the limits on what a corporate network will access on the user client device has changed;

providing an updated version of the limits on what a corporate network will access on the user client device; and

providing the client access to the corporate network by the server once the user has accepted the updated version of the limits on what a corporate network will access on the user client device.

17. The non-transitory computer readable storage medium of claim **12**, further comprising:

providing the user with information regarding what applications have sent data to the corporate network; and

providing an indication of compliance to the user regarding whether the data sent by the applications complies with the user agreement on what a corporate network will access on the user client device.

18. The non-transitory computer readable storage medium of claim **12**, further comprising:

providing an administrator of the corporate network with information regarding what applications have sent data to the corporate network; and

providing an indication of compliance to the administrator regarding whether the data sent by the applications complies with the user agreement on what a corporate network will access on the user client device.

19. The non-transitory computer readable storage medium of claim **12**, further comprising providing a list of applications allowed to access the corporate network to the user, the list provided from the server to the user through the user client device.

20. The non-transitory computer readable storage medium of claim **19**, further comprising receiving input from the user to select a subset of the list of applications to access the corporate network, wherein the one or more applications not selected by the user are blocked access to the corporate network.

21. The non-transitory computer readable storage medium of claim **19**, wherein the list is provided to the user at the start of the connection between the user client device and the server.

22. The non-transitory computer readable storage medium of claim **21**, further comprising:

detecting during the connection a change to the list of applications allowed to access the corporate network; and

providing the user with an updated list of applications allowed to access the corporate network.

23. A device for establishing a connection with a remote server, the device including:

a processor;

memory;

an agent stored in memory and executed by the processor to establish a connection between a user client device and a server, the user client device having a plurality of applications and associated with a user, present to the user through the user client device a user agreement on what a corporate network will access on the user client device, receive a confirmation of the user agreement from the user by the client device, and provide the client access to the corporate network.

24. The device of claim **23**, further comprising generating the user agreement for the user and user client device combination.

25. The device of claim **23**, further comprising storing the user acceptance of the user agreement for the user and user client device combination by the server.

26. The device of claim **23**, further comprising providing the user agreement to the user subsequent to the providing the client access to the corporate network by the server.

27. The device of claim **23**, further comprising:

receiving login information from the user by the server via the user client device;

determining if the limits on what a corporate network will access on the user client device has changed;

providing an updated version of the limits on what a corporate network will access on the user client device; and

providing the client access to the corporate network by the server once the user has accepted the updated version of the limits on what a corporate network will access on the user client device.

28. The device of claim **23**, further comprising:

providing the user with information regarding what applications have sent data to the corporate network; and

providing an indication of compliance to the user regarding whether the data sent by the applications complies with the user agreement on what a corporate network will access on the user client device.

29. The device of claim **23**, further comprising:

providing an administrator of the corporate network with information regarding what applications have sent data to the corporate network; and

providing an indication of compliance to the administrator regarding whether the data sent by the applications complies with the user agreement on what a corporate network will access on the user client device.

30. The device of claim **23**, further comprising providing a list of applications allowed to access the corporate network to the user, the list provided from the server to the user through the user client device.

31. The device of claim **30**, further comprising receiving input from the user to select a subset of the list of applications to access the corporate network, wherein the one or more applications not selected by the user are blocked access to the corporate network.

32. The device of claim **30**, wherein the list is provided to the user at the start of the connection between the user client device and the server.

33. The device of claim **32**, further comprising:

detecting during the connection a change to the list of applications allowed to access the corporate network; and

providing the user with an updated list of applications allowed to access the corporate network.

* * * * *